**IT Applications, Unit 4**

**Security and ethical considerations, Ch 8, p 285**

Security Equipment

**Security hardware**

1. What is meant by data integrity?

The assurance that data is accurate and reliable, and is available in a timely manner

1. Biometrics
   1. Describe biometric security.

Authentication based on the use of human characteristics

* 1. Why does it appeal to security managers?

it is nearly impossible to copy or steal a person's biometric devices

* 1. List the common biometric devices.

voice recognition

fingerprint recognition

hand geometry

signature verification

facial recognition

iris recognition

* 1. What are the concerns of biometric technology?

1. Swipe cards
   1. Describe the nature of a swipe card.
   2. What is a limitation of the swipe card?
2. Smart cards
3. Security tokens
4. Mobile phone secure code
   1. How does this level of authentication work?

**Power protection**

Outline the characteristics of the following:

1. Surge protector
2. Uninterruptible power supply, (UPS)

**Strategies for avoiding system failure, p 288**

1. What is meant by redundancy?
2. What is meant be a fault-tolerant server?
3. Redundancy through multiple hard drives or fault-tolerant equipment
   1. Describe how this redundancy works.
   2. What is meant by RAID technology
4. Redundancy through mirrored servers or machines
   1. Why is the RAID solution preferable to this solution?

**Backup Media**

1. There are a range of options for backup media, what 3 factors should be considered when deciding on which backup media to use?

Three categories of backup media:

List the characteristics of the following backup media:

**Magnetic media**

1. hard disk drive
2. Magnetic tapes

**Optical media**

1. Compact disc
2. DVD
3. Blu-ray

**Solid-state drives**

1. USB storage devices

**Online backups**

1. Why do organisations use this form of backup?
2. Describe an enterprise storage system.

**Surveillance technology, p 292**

Describe the nature of the following items of surveillance equipment used in offices:

1. Packet sniffers
2. Desktop monitoring programs
3. Log files
4. Closed-circuit television, (CCTV)
5. Telephones
6. Audit trails

**Physical security devices:** List the options for physically securing your data